(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 April 2002 (18.04.2002)

PCT

(10) International Publication Number
WO 02/31718 A1

(51) International Patent Classification[7]: G06F 17/60, H04L 9/32

(21) International Application Number: PCT/FI01/00878

(22) International Filing Date: 10 October 2001 (10.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20002234 10 October 2000 (10.10.2000) FI

(71) Applicant *(for all designated States except US)*: **SONERA SMARTTRUST LTD** [FI/FI]; Elimäenkatu 17 - 19, FIN-00510 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PIETILÄINEN, Henna** [FI/FI]; Nostovaenkuja 7 C 3, FIN-02660 Espoo (FI). **KOLSI, Otto** [FI/FI]; Alkutie 6-8 B 7, FIN-00660 Helsinki (FI). **LEHTONEN, Veera** [FI/FI]; Merimiehenkatu 39 B 42, FIN-00150 Helsinki (FI). **MÄTTÖ, Mikko** [FI/FI]; Jämeräntaival 5 B 216, FIN-02150 Espoo (FI).

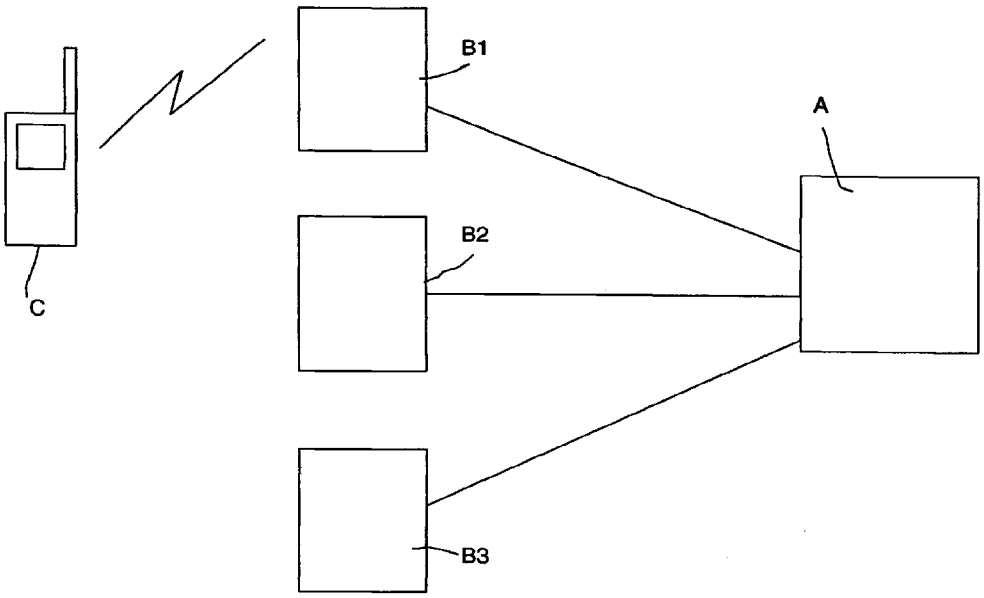
(74) Agent: **PAPULA OY**; P.O. Box 981, (Fredrikinkatu 61 A), FIN-00101 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: METHOD FOR USING SERVICES IN A WIRELESS COMMUNICATION NETWORK



(57) Abstract: The invention is concerned with a method and a wireless communication network for using trusted services. The network comprises a service provider, one or moreservice devices and one or more mobile stations. Digital signatures are used in thecommunication between the parties for identity verification. In the method, information messages are created creating by the service provider. The messages are digitallysigned to prove the identity of the sender. Said signed messages are then sent to one or more of the service devices and stored therein. From the service device(s), the signed messages are sent to one or more of the mobile stations for further communication.

WO 02/31718 A1

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD FOR USING SERVICES IN A WIRELESS COMMUNICATION NETWORK

TECHNICAL FIELD

The invention relates to a method and communication network for using trusted services.

BACKGROUND ART

Recent developments in information system technology have created new marketing opportunities. With improved technology available to reach customers at home and business places, interactivity becomes a greater issue.

There are, however, not yet any direct point-of-sale locations having information system techniques with interactive capabilities for use by advertisers and others.

An example of a prior art point-of-sale solution is the US patent 5,642,484, which provides a point-of-sale information distribution and presentation system which is centrally controlled. The system comprises intelligent automated devices at the point-of sale locations, which may be coupled e.g. to a satellite, land line etc. Moreover, these systems may be arranged to alter the distribution or presentation of the information according to environment sensing information at point-of-sale level. In this patent, automated devices are linked e.g. via a satellite to a service bureau, which in turn is connected to an information provider. The service bureau is adapted to receive data relating to the actual presentation of the information advertisements. The system has sensors to detect approaching customers. This system, however, lacks interactive capabilities with the customer.

Moreover, known systems for point-of sale advertising and subsequent responding are, however, not secure as the identity of the parties in the system can not be verified.

In communication systems, security can be introduced by e.g. using known Public Key Infrastructures for encrypting messages, creating digital signatures and for verifying the signature of a sender of a message.

The principle of such infrastructures can be that everyone in the communication system has a public key, that is known for everyone in the system and which is used to encrypt messages, and a private key for decrypting messages that are encrypted with the public key.

A common way of proving an identity is to use a signature. If a message instead is encrypted with the private key, the message can be decrypted with the public key. The idea of signing messages with the RSA system is encryption with the private key and decryption with the public key, in which case it is certain that only the holder of the private key could have sent that message. Thus, a key pair can be used in an opposite direction for digitally signing of messages in such a way that a message is signed with the private key (the message or a part of it is encrypted with the private key) and the signature is verified with the public key (by decrypting with the public key). In practice it is only a digest of the message that is encrypted with the private key to avoid overlong messages.

To be sure that the recipient really knows that the right person holds the private key, the particular key has to be bound to an individual or corporation in some way. For this purpose, a third party is used to certify that the public key belongs to the owner. The binding of identity to a particular key pair is done using a certificate that attests to the owner's identity. This certificate must be issued by a certification authority (CA), which is an organization that verifies identities and issues certificates that bind key pairs to identities. A certificate lists at least the owner of the key pair, often the organization of the owner, the owner's public key, expiration information and a digital signature created using the CA's private key. The public keys of the CAs are usually built into the applications that use public key systems, so the software can validate the certificate. More detailed information about the technology involved in public key infrastructure systems can be found e.g. in the book "Understanding Digital Signatures" by Gail L. Grant, ISBN 0-07-012554-6.

The object of the invention is a secure method for distributing trusted messages in wireless communication networks via an intermediate device.

A more detailed object for the secure method of the invention is to obtain security in such networks without the need for special protection for the intermediate device.

SUMMARY OF THE INVENTION

The method of the invention uses trusted services in a wireless communication network, which comprises a service provider, one or more service devices and one or more mobile stations. The identity of the sender of messages in the communication between the parties is verified by means of digital signatures. In the method, information messages are created by the service provider. After proving of the identity of the sender in said messages by digitally signing the messages, said signed messages are sent and stored in one or more of the service devices. The signed messages are then sent from the service device(s) to one or more of the mobile stations for further communication.

The service provider has means for creating information messages and for digitally signing said messages, the service device(s) has means for sending and storing said signed messages, and the mobile station(s) has means for verifying the signed messages received. The mobile station has also means for digitally signing of the messages and for verification of certificates.

The identity verification is advantageously performed by means of a public key infrastructure using public and private keys as well as certificates for the signing of the messages sent in the method.

The method of the invention is advantageously performed by making use of a Public Key Infrastructure: The following keys are stored in the components making up the wireless network of the invention.

The service provider and the mobile stations have their private keys for signing messages. The mobile stations have or have availability to the public key of the service provider for checking the digital signatures of messages sent from the service provider and forwarded by the service devices. The mobile station(s) also has availability to a certificate that binds its keys to themselves thus to prove their identity. A merit of the invention is that the service devices do not need to have any own keys, as they only forward the information messages from the service providers to the mobile stations. The only key needed to be stored in the service device is the public key of the CA. The service device also gets the certificate of a mobile station intending to make an order.

The invention can be used in service devices without any secret keys and with a data communication connection that does not have to be continuous. The service devices of the invention can verify the sender of the signed messages by means of the public key of the CA stored therein. Furthermore, the service devices can be used to store data about the users that have used the service and to store digital signatures.

In the advantageous embodiment, wherein the device has no secret keys, the merit of the invention is that cheaper devices can be used as they are not so exposed to misuse and attacks and are thus less critical.

Thanks to the signed messages sent from the service provider, the devices can advertise their own services for users in a trusted way so that the users can be sure that the advertisements are from the right service providers/devices indicated in the messages.

The sender of the message can be identified by means of the digital signature. The messages can not be later denied and thus they can be used for charging.

The processing power of the devices of the invention and the memory capacity can be compared with those of a smart card and if desired, the functionality as a whole can be performed by means of a smart card.

Depending on the memory capacity of the service device, a different message can be sent every time, whereby no special counters are needed to avoid replay attacks.

If a more extensive data connection between the service provider and the service devices is used, the mobile terminal using the services does not need to send its own certificate to the device as the device can fetch it in the network from a certificate director. If it is question about a service for a limited number of users, the certificates of all possible users can be stored in the device in alternative to the embodiment in which the mobile terminal sends it certificate in connection with the use of the service.

It is also possible to use an advertisement, which can be changed by the user, in which case the receiver can tell the desired content of the service used.

In the following the invention will be described by means of figures and examples of some advantageous embodiments. The invention is not limited to the details of the embodiments or to the services used therein.

FIGURES

Figure 1 is an example of an environment in which the invention can be performed.
Figure 2 is a flow scheme of an example of how the invention can be performed.
Figure 3 is an illustration about an example of service and how it can be used with the invention

DETAILED DESCRIPTION

Figure 1 illustrates an example of an environment in which the invention can be performed. The communication system of the invention comprises in figure 1 a service provider A, service devices B1, B2 and B3 and mobile stations C. The mobile

station is preferably a mobile phone. However, it can be any temper proof mobile device. In addition to the components appearing in figure 1, a certificate director usually belongs to the communication system. The mobile stations are connected to the service devices with e.g. radio links and the service devices can be connected to the service provider with, e.g. cable links, optical fibres, or radio links including Bluetooth radio links.

The system of figure 1 can make use of a Public Key Infrastructure to secure a trusted communication between the parties belonging to the system. For that purpose, the service provider stores its own private key, with which it can sign messages digitally. Also the mobile stations can sign messages with their own private keys. Anyone in the system has access to the public keys of the mobile station and the service provider to check digital signatures created by means of the respective private keys. There are key pairs also for encrypting and decrypting messages. The mobile stations and the service providers in the system also have certificates by means of which their identity can be verified. The public keys, by means of which the identities can be verified, are included in these certificates that can be fetched from a certificate directory or they can be stored in the components. A certification authority CA keeps records about key pairs and their owners. The service devices do not have any own private keys, but they have the public key of a certification authority CA stored therein to check certificates sent to them.

A is a service provider that owns the service devices B1, B2 and B3. The service provider A might as an example offer parking services, in which case B1, B2 and B3 can be parking measuring units or refreshment units in which case the service devices can be lemonade automates. Other examples of services might be candy automates, ticket automates, gate entrances etc.

The idea of the invention is to enable the service devices to inform about their services to the mobile stations in a secure way so that the mobile users can be sure about who the sender of the messages is. The mobile station also has to be sure about that it is secure to order the service offered in the messages without the risk of replay attacks.

An example of how the invention can be performed e.g. in the environment of figure 1 is shown in figure 2.

A service provider creates an information message, e.g. an advertisement in step 1. To prove its identity, the service provider signs the message digitally in step 2 and sends 3 the signed message to one or more service devices B. The message sent from the service provider is stored 4 and thereafter sent 5 to one or more mobile stations C.

The message might be an advertisement for a parking service, for buying products, for participating in a questionnaire or other such service.

The message can appear 6 in the mobile station C in different ways, such as a short message (SMS). The service device B may also be a cellular base station. The message can be a cell broadcast message or other message when the mobile station C enters a certain cell area or other specified area.

If the mobile station decides to respond to the message, e.g. by requesting additional information, making an order or by answering questions or sending a report, a response message is created 7. For identity verification, the mobile station can send its certificate to the service device in step 8 which, however, in that case usually is sent before creating the message in step 7. The certificate has been signed with the private key of the CA. The service device B can now check the certificate by means of the public key of the CA. Upon approval 9 of the certificate, which is indicated for the mobile station in step 10, the mobile station C digitally signs 11 the response with the private key of the mobile station and sends 12 it to the service device B. Alternatively, the service device might already have the certificate of the mobile station stored and in that case steps 8 – 10 are omitted. This might be the case e.g. if the service is intended for a limited user group known in advance, in which case it is possible to store all or a part of the necessary certificates in the service device in advance. Another alternative is that the service device fetches the certificate of the mobile station from a certificate directory of the CA if it has such connection.

Now the mobile station can respond to the message received from the service device in step 6 and creates the response in step 7, which can e.g. include an order of a service. The response is digitally signed by the mobile station in step 11 with its private key to prove its origin.

The service device can check the digital signature by means of the certificate of the mobile station. When the signature has been approved 13, the service device can perform 14 the service informed about in the information message and ordered by the mobile station.

Information about the use of services can be sent 15 to the service provider A from the service device B, which can use the information e.g. to charge the client or as an information source for further communication strategies.

The invention also provides solutions to prevent replay attacks, wherein the above mentioned order message from the mobile station to the service device is stored by someone to be repeatedly used.

Firstly, the service provider can store different advertisements or information messages in the different service devices. Each such message contains a date and a time stamp or some other changing information, e.g. a new information for every hour.

Every service order message has a unique message number and the time stamp that was in the information message of the device. The device stores pairs constituted by a MS (Mobile Station) identity and a message number. The order message is accepted if it contains the actual time stamp and a new pair of message number and MS identity. The message is changed e.g. every hour and the message numbers are deleted from the database.

CLAIMS

1. Method for using trusted services in a wireless communication network, comprising a service provider, one or more service devices and one or more mobile stations, in which method digital signatures are used in the communication between the parties for identity verification,
   characterized by
   a) creating information messages by the service provider,
   b) digitally signing the messages to prove the identity of the sender of said messages,
   c) sending said signed messages from the service provider to one or more of the service devices and storing the signed messages therein,
   d) sending the signed messages from the service device(s) to one or more of the mobile stations for further communication.

2. Method of claim 1, characterized in that the identity verification is performed by means of Public Key Infrastructure.

3. Method of claim 2, characterized in that the digital signing in step b) is performed with the private key of the service provider.

4. Method of claim 1, characterized in that the further communication takes place by sending from the mobile station, a response to the message received by
   e) sending the certificate of the mobile station to the service device,
   f) approving the certificate at the service device, and
   g) sending the response from the mobile station to the service device by digitally signing the message with the private key of the mobile station.

5. Method of claim 4, characterized in that the digital signature in step e) is made by the private key of the CA.

6. Method of claim 4, characterized in that the digital signature in step g) is made by the private key of the mobile station.

7. Method of claim 1, c h a r a c t e r i z e d in that the further communication takes place by responding to the message from the mobile station by
   e) sending the response from the mobile station to the service device by digitally signing the message with the private key of the mobile station,
   f) approving the response at the service device by means of the certificate of the mobile station.

8. Method of claim 7, c h a r a c t e r i z e d in that the service device fetches the certificate of the mobile station from a certificate directory.

9. Method of claim 7, c h a r a c t e r i z e d in that the certificate of the mobile station is stored at the service device in advance.

10. Method of claim 4, c h a r a c t e r i z e d in that the response from the mobile station to the service device is an order of a service provided by the service provider.

11. Method of claim 4, c h a r a c t e r i z e d by a still further communication in which the response is approved at the service device and the service ordered by the mobile station in its response is performed by the service device.

12. Method of claim 4, c h a r a c t e r i z e d in that the digital signature in step g) is checked by the service device by using the certificate of the mobile station.

13. Method of claim 1, c h a r a c t e r i z e d in that the information messages sent to the service devices from the service provider differ from each other.

14. Method of claim 1, c h a r a c t e r i z e d in that each information message contains a date and/or time and/or a number.

15. Method of claim 4, c h a r a c t e r i z e d in that the service devices keep record about the responses sent to them from the mobile stations.

16. Method of claim 12, c h a r a c t e r i z e d in that the records contain information about the mobile clients, as well as the date and time stamps.

17. Method of claim 1, c h a r a c t e r i z e d in that each service device receives more than one information message from the service provider.

18. Method of claim 1, c h a r a c t e r i z e d in that the information message to be sent from the service device to the mobile station is regularly changed.

19. Method of claim 18, c h a r a c t e r i z e d in that each such information message contains a date and a time stamp or some other changing information for every hour.

20. Method of claim 18, c h a r a c t e r i z e d in that every service order message has a unique message number and the time stamp that was in the information message of the device.

21. Method of claim 20, c h a r a c t e r i z e d in that reply attacks are avoided by storing pairs constituted by a MS (Mobile Station) identity and a message number, and by only accepting service order messages that contain the actual time stamp and a new pair of message number and MS.

22. Wireless communication network, comprising a service provider, one or more service devices, one or more mobile stations, and means for identity verification of the parties in the communication, c h a r a c t e r i z e d in that

a) the service provider has means for creating information messages and for digitally signing of the messages,

b) the service device(s) has means for sending and storing said signed messages,

c) the mobile stations have means for verifying the signed messages received and for digitally signing messages to be sent.

23. Wireless communication network of claim 19, c h a r a c t e r i z e d in that the means for identity verification is Public Key Infrastructure using public and private keys as well as certificates for the signing of the messages sent in the method.

24. Wireless communication network of claim 20 or 21, c h a r a c t e r i z e d in that it also comprises a certificate directory of a CA.

25. Wireless communication network of any of claims 19 -21, c h a r a c t e r i z e d in that the service devices have the public key of the CA.

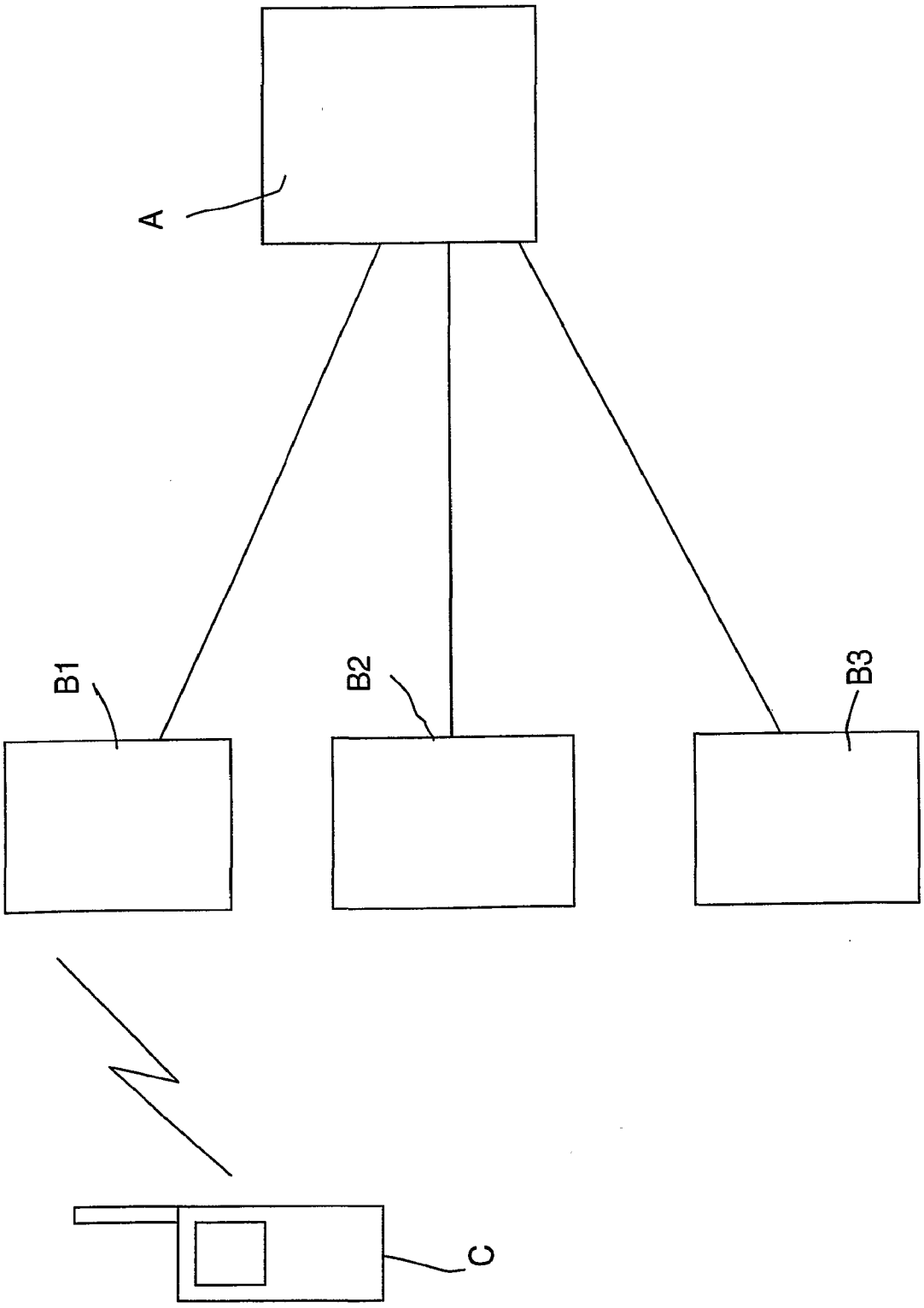


FIG. 1

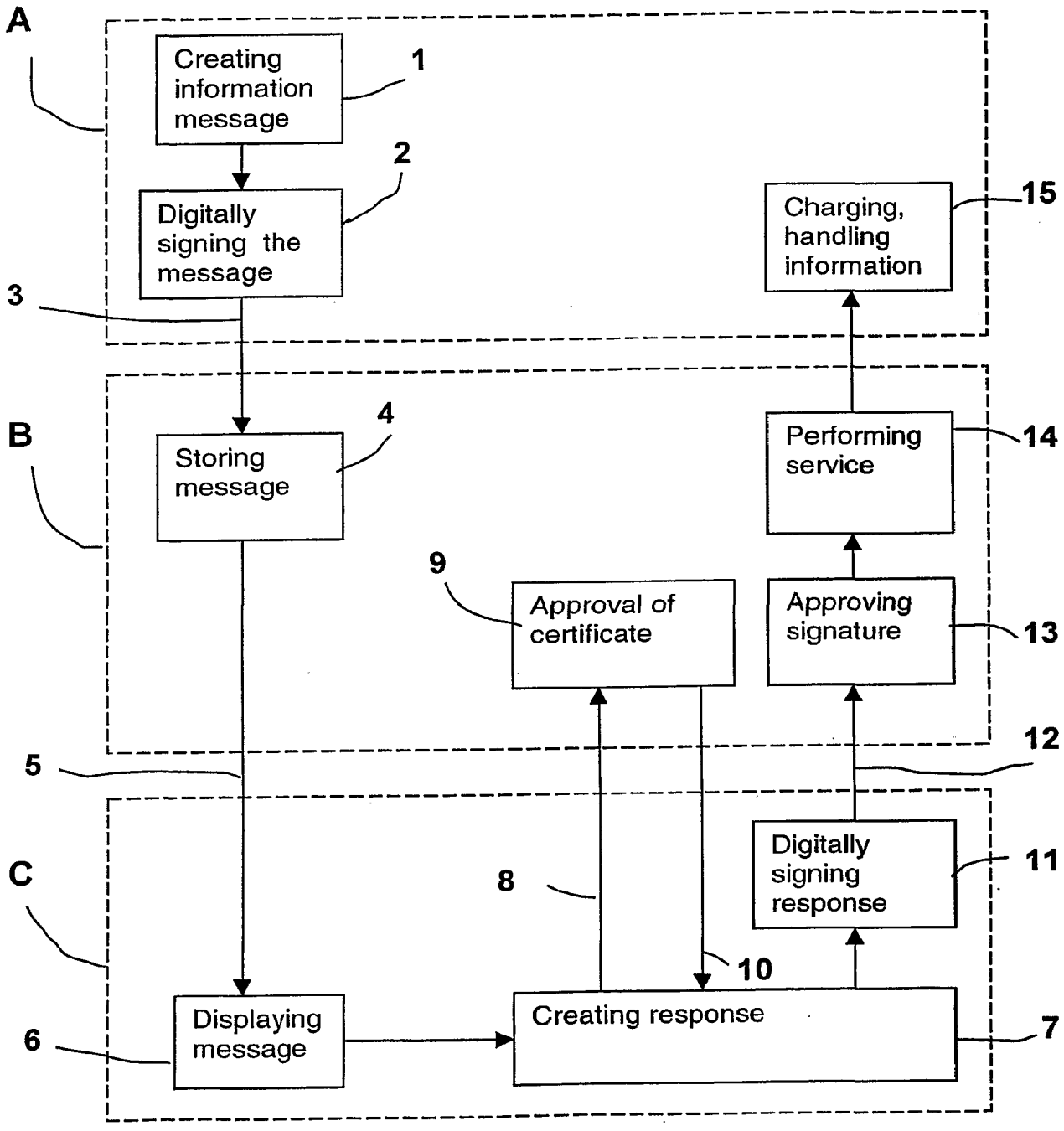

A
Creating information message
1
2
Digitally signing the message
3
Charging, handling information
15
B
4
Storing message
Performing service
14
9
Approval of certificate
Approving signature
13
12
5
C
8
Digitally signing response
11
10
Displaying message
6
Creating response
7

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00878

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/60, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI DATA, EPO INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5592560 A (D.W. DEATON ET AL.), 7 January 1997 (07.01.97), abstract ---	1-2,4,7, 13-14,17-18
P,X	EP 1077437 A2 (PHONE. COM. INC.), 21 February 2001 (21.02.01), figure 1, abstract ---	1-2,4,7, 13-14,17-18
A	US 5757918 A (W.D. HOPKINS), 26 May 1998 (26.05.98), column 1, line 63 - column 2, line 15 ---	1-2,4,7, 13-14,17-18
A	US 5926796 A (J.S. WALKER ET AL.), 20 July 1999 (20.07.99), see the whole document ---	1-25

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 January 2002	29-01-2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00878

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5642484 A (N.C. HARRISON, III ET AL.), 24 June 1997 (24.06.97), see the whole document -- --------	1-25

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 01/00878

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5592560 A	07/01/97	US 5388165 A	07/02/95
		US 5327508 A	05/07/94
		US 5201010 A	06/04/93
		US 5237620 A	17/08/93
		US 5305196 A	19/04/94
		US 5430644 A	04/07/95
		US 5448471 A	05/09/95
		US 5621812 A	15/04/97
		US 5638457 A	10/06/97
		US 5642485 A	24/06/97
		US 5644723 A	01/07/97
		US 5649114 A	15/07/97
		US 5659469 A	19/08/97
		US 5675662 A	07/10/97
		US 5687322 A	11/11/97
		US 6307958 B	23/10/01
EP 1077437 A2	21/02/01	CN 1280344 A	17/01/01
		JP 2001076058 A	23/03/01
US 5757918 A	26/05/98	CA 2167631 A	21/07/96
		EP 0723251 A	24/07/96
US 5926796 A	20/07/99	AU 6771498 A	20/10/98
		BR 9815463 A	06/11/01
		CN 1253644 T	17/05/00
		EP 1016012 A	05/07/00
		IL 131143 D	00/00/00
		US 6317723 B	13/11/01
		WO 9843149 A	01/10/98
US 5642484 A	24/06/97	NONE	